

SD:FJN
F.#2019R00408

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF
ELECTRONIC DEVICES CURRENTLY
LOCATED IN THE CUSTODY OF THE
DRUG ENFORCEMENT
ADMINISTRATION

APPLICATION FOR A SEARCH
WARRANT FOR ELECTRONIC
DEVICES

Case No. 20-M-198

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, David C. Brown, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Drug Enforcement Administration (“DEA”). I have been a DEA Special Agent for approximately 8 years and am currently assigned to the New York Division. During my tenure with the DEA, I have participated in numerous investigations of drug trafficking organizations during which I have conducted physical and electronic surveillance, executed court-authorized search warrants, debriefed cooperating witnesses and victims, reviewed and analyzed numerous taped conversations of those

engaged in illegal activity, monitored wiretapped conversations and reviewed line sheets prepared by wiretap monitors. Through my training, education and experience, I have become familiar with the manner in which drug trafficking schemes are carried out and the efforts of persons involved in each activity to avoid detection by law enforcement. I have also become familiar with the way that electronic devices, including cellular telephone, computers, and storage devices are used in furtherance of criminal activity.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched are as follows:
- a. A black Apple iPhone cellular telephone seized from Gilbert Cardenas on or about February 4, 2020 and currently in DEA custody as Exhibit N-7 in File No. C1-19-0020 (“Device 1”);
 - b. A silver Apple iPhone cellular telephone seized from Rogelin Florian on February 4, 2020, bearing IMEI number 3557850731333263 and currently in DEA custody as Exhibit N-8 in File No. C1-19-0020 (“Device 2”); and

- c. A rose gold Apple iPhone cellular telephone seized from Rogelin Florian on February 4, 2020 and currently in DEA custody as Exhibit N-9 in DEA File No. C1-19-0020 (“Device 3”);
5. Devices 1-3 (collectively the “Devices”) are currently located in the custody of the DEA in the Eastern District of New York.
6. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

7. Beginning in December 2019, the DEA and the New York City Police Department (“NYPD”) used an NYPD confidential informant (“CI”) to conduct undercover cocaine base (i.e. crack cocaine) purchases from Gilbert Cardenas (“Cardenas”). Successful undercover buys took place in December 2019 and January 2020. During those buys, officers observed an unidentified Hispanic male who appeared to be working with Cardenas to distribute the crack cocaine. In order to identify and arrest Cardenas and the unidentified male, the officers arranged a third undercover buy, as explained below.
8. On or about February 3, 2020, the CI, acting at the direction of law enforcement, contacted Cardenas via text message and arranged to purchase 56 grams of

crack cocaine from Cardenas the following day for a previously negotiated amount of \$2,020.¹

9. On or about February 4, 2020, Cardenas instructed the CI via text message to meet Cardenas at Cardenas' apartment in Brooklyn, New York at 3 p.m.

10. At approximately 2:45 p.m., the CI met with DEA and NYPD officers at a location in Brooklyn, New York. The officers searched the CI for contraband with negative results. The officers then handed the CI \$2,020 in United States currency to purchase the crack cocaine (the "Buy Money"). Prior to giving the Buy Money to the CI, officers recorded the serial numbers on the currency. The officers also equipped the CI with audio and video recording devices. Officers then established surveillance in anticipation of the CI's meeting with Cardenas.

11. At approximately 3:00 p.m., officers observed the CI walk towards Cardenas' apartment on Pacific Street in Brooklyn New York and then enter the building containing Cardenas' apartment (the "Apartment Building").

12. At approximately 3:10 p.m., officers observed a blue Honda Odyssey driven by Cardenas arrive at the location. Shortly thereafter, officers observed the CI exit the Apartment Building and enter the back seat of the Honda Odyssey. Once the CI was inside the Honda Odyssey, the CI observed Cardenas place a telephone call in Spanish using

¹ The NYPD previously arrested the CI for distributing crack cocaine. The CI is cooperating with law enforcement in the hope of obtaining leniency for his narcotics trafficking. The information provided by the CI has proven reliable in the past and has been corroborated by independent investigative techniques.

Device 1, which, as discussed below, officers later recovered from Cardenas. After completing the telephone call, Cardenas told the CI that his source was on the way.

13. At approximately 3:34 p.m., officers observed an individual, later identified as Rogelio Florian (“Florian”), walk on Pacific Street and enter the Apartment Building. The CI reported that once Florian arrived, Cardenas asked the CI for the money for the crack cocaine. At that point, the CI handed over the Buy Money. Immediately thereafter, officers observed Cardenas exit the Honda Odyssey and enter the Apartment Building. Moments later, officers observed Cardenas exit the Apartment Building and re-enter the Honda Odyssey. The CI reported that upon re-entering the Honda Odyssey, Cardenas handed the CI a black bag containing two smaller plastic bags containing crack cocaine. Meanwhile, officers also observed Florian exit the Apartment Building and walk on Pacific Street.

14. At this time, officers approached Florian and arrested him. At the same time, other officers approached the Honda Odyssey, arrested Cardenas, and detained the CI. A search incident to arrest of Florian revealed \$1,820 of the Buy Money in Florian’s left jacket pocket, as well as Device 2 and Device 3. A search incident to arrest of Cardenas revealed \$200 of the Buy Money and Device 1. A search of the CI revealed a black bag containing two smaller plastic bags containing crack cocaine. Based on my training and experience, Florian is Cardenas’s crack cocaine supplier and Cardenas used Device 1 to contact Florian via Device 2 and/or Device 3 in the presence of the CI, as described above. Based on this contact, Florian showed up at Apartment Building, in possession of crack cocaine, Device 2, and Device 3, and met up with Cardenas to exchange drugs for cash. As a result of this

meeting and exchange, both Florian and Cardenas had some of the Buy Money in their possession when they were arrested.

15. I know that the Devices have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the Devices first came into the possession of the DEA.

TECHNICAL TERMS

16. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading

information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.
- c. Portable media player: A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

- d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna’s latitude, longitude, and sometimes altitude with a high level of precision.
- e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital

data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system (“GPS”) technology for determining the location of the device.

- f. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

17. Based on my training, experience, and research, I know that the Devices have capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS, PDA, and/or computer. I further know that the Devices can be used to store data and/or access the internet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device, as well as who had been in contact with the Device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

18. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

19. There is probable cause to believe that things that were once stored on the Devices may still be stored there, for at least the following reasons:

- a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application

operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

20. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment

of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

- f. I know that when an individual uses an electronic device to illegally sell controlled substances, the individual's electronic device will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic device is an instrumentality of the crime because it is used as a means of committing the criminal offense. The electronic device is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that an electronic device used to commit a crime of this type may contain: data that is evidence of how the electronic device was used; data that was sent or received; and other records that indicate the nature of the offense.

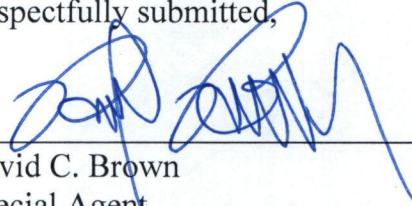
21. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

22. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

23. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,



David C. Brown
Special Agent
Drug Enforcement Administration

Subscribed and sworn to before me
on February 26, 2020:



THE HONORABLE ROBERT M. LEVY
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

UNITED STATES DISTRICT COURT

for the
Eastern District of New York

In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address)) Case No. 20-M-198
Electronic Devices Currently Located in the Custody)
of the Drug Enforcement Administration)

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the Eastern District of New York
(identify the person or describe the property to be searched and give its location):

See Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B.

YOU ARE COMMANDED to execute this warrant on or before March 11, 2020 (not to exceed 14 days)
☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the Duty Magistrate Judge
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for days (not to exceed 30) ☐ until, the facts justifying, the later specific date of .

Date and time issued: February 26, 2020 at 8:16 p.m.

Robert Levy
Judge's signature

City and state: Brooklyn, New York

Hon. Robert M. Levy U.S.M.J.
Printed name and title

ReturnCase No.:
20-M-198

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

*Executing officer's signature*_____
Printed name and title

ATTACHMENT A

The property to be searched are as follows:

- a. A black Apple iPhone cellular telephone seized from Gilbert Cardenas on or about February 4, 2020 and currently in DEA custody as Exhibit N-7 in File No. C1-19-0020 (“Device 1”);
- b. A silver Apple iPhone cellular telephone seized from Rogelin Florian on February 4, 2020, bearing IMEI number 3557850731333263 and currently in DEA custody as Exhibit N-8 in File No. C1-19-0020 (“Device 2”); and
- c. A rose gold Apple iPhone cellular telephone seized from Rogelin Florian on February 4, 2020 and currently in DEA custody as Exhibit N-9 in DEA File No. C1-19-0020 (“Device 3”);

Devices 1-3 (collectively the “Devices”) are currently located in the custody of the DEA in the Eastern District of New York. This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Devices described in Attachment A that relate to violations of 21 U.S.C. §§ 841 and 846 and involve Rogelin Florian or Gilbert Cardenas since December 1, 2019, including:

- a. Any subscriber information or contact information, to include names, addresses, telephone numbers, email addresses, or other identifiers located in a contact list, telephone book, or otherwise;
- b. Any call log information, including missed, incoming, and outgoing calls, and any information associated with those telephone numbers;
- c. Any photographs, videos, and audio files;
- d. Any text messages, email messages, chats, multimedia messages, WhatsApp messages, installed applications, or other electronic communications;
- e. Any calendar, note, or password entries;
- f. Any internet or browser entries or history;
- g. Any system, data, or configuration information contained within the Devices, including but not limited to the phone number of the Devices;
- h. Any information regarding types, amounts, and prices of drugs trafficked as well as dates, places, and amounts of specific transactions;

- i. Any information related to sources of drugs (including names, addresses, phone numbers, or any other identifying information)
 - j. Any information regarding Rogelin Florian or Gilbert Cardenas' schedule or travel from December 1, 2019 to the present;
 - k. All communications between Rogelin Florian and Gilbert Cardenas.
2. Evidence of user attribution showing who used or owned the Devices at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.